



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,010	02/26/2002	Matthew Charles Priestley	MS190438.1	4314

27195 7590 12/07/2006

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER

ABEDIN, SHANTO

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 12/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/083,010	Applicant(s) PRIESTLEY ET AL.	
	Examiner Shanto M Z Abedin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 September 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-18,20-29 and 31-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-18,20-29 and 31-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the amendment filed on 09/28/2006.
2. Claims 2, 19 and 30 are previously cancelled by the applicant.
3. Claims 1, 3-18, 20-29 and 31-33 are pending in the application.
4. Claims 1, 3-18, 20-29 and 31-33 have been rejected.

Response to Arguments

5. Regarding the USC 103 rejections of claims 1, 3-18, 20-29, 31-33, the applicant primarily argues that Lee et al, Hypponen, or Bathrick, or Brainard individually or combined does not teach:

(a) a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key; the applicant further adds “the pass-phrase taught by Hypponen is used to generate a cryptographic key that allows access to encrypted data in a computer device. The pass-phrase is not employed in connection with generation of the cryptographic wrapper. Therefore, Hypponen is silent regarding a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key.”; and

(b) the pass-phrase distributed separately from the credentials; the applicant further adds “the noted password of Bathrick et al is not equivalent to the claimed pass-phrase. The password in the reference is a mechanism to protect transferred data. On the contrary, a pass-phrase generates wrapper of a password, where the passphrase is needed to access the wrapper”

In response to applicant's above argument (a), the examiner respectfully disagrees with the applicant for the following reasons:

Firstly, the claim limitations recite “generation of the wrapper via a cryptographic wrapping key” which can be interpreted as generation of a cryptographic wrapping key which works as/ is a wrapper. The applicant contends that Hypponen teaches generation of a cryptographic key, not a

Art Unit: 2136

wrapper. However, Hypponen also teaches such cryptographic key derived from a passphrase is a “lock” for the file access (Hypponen, Background of the invention, line 17-28) similar to what disclosed in the specification of the present application (Page 8, lines 1-20; passphrase to lock/ unlock the package). Therefore, Hypponen’s cryptographic key is a wrapping/ locking key, or a wrapper/ lock that is derived from a pass-phrase.

Secondly, even for the sake of arguments if it is believed that Hypponen’s cryptographic key is not a wrapper, or not part of generation of a wrapper, the examiner likes to point out that generation of such wrapper using a passphrase or cryptographic function is already taught by the reference Lee et al (Section 2.2 and 3.2; Lee et al teaches unlocking mechanism for a wrapped software/ package, or a wrapper using an electronic license containing a cryptographic function derived from a pass-phrase/shared secret, therefore, Lee’s cryptographic function in a e-license can be thought of a wrapping/ unwrapping, or locking/ unlocking key). Therefore, the **combination** of the Hypponen and Lee et al does teach a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key.

In response to applicant’s above argument (b), the examiner respectfully disagrees with the applicant for the following reasons:

The claim limitations of the instant application recite “a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service” which can be interpreted as pass-phrase is a keying material, and also can be used to lock/ unlock the credentials. The applicant argues that Bathrick discloses a password rather than a pass-phrase that is distributed separately from the credential. However, Bathrick’s “password” is a keying

Art Unit: 2136

and/ or certificate material, and also a “shared secret” that is used for both integrity and encryption to protect data (Bathrick, Col 1, lines 23-47; Col 2, lines 18-40).

The applicant further argues that “the password in the reference is a mechanism to protect transferred data. On the contrary, a pass-phrase generates wrapper of a password, where the passphrase is needed to access the wrapper”. In response to the applicant's above argument, it is noted that the features upon which applicant relies such as “a pass-phrase generates wrapper of a password,” is not recited in claim 1. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). For that reason, above argument is not at least valid for claim 1.

Furthermore, according to Bathrick, the motivation for sending such password/ keying material/ shared secret separate from the certificate/ keys/ credentials is communication/ data protection (Batherick, Col 1, lines 23-47) is same as the motivation set forth in the specification of the present application for the separate delivery of the pass-phrase and credential (Page 8, line 12-15, communication security). Therefore, Batherick’s password also can be thought of as a shared secret or key material, or at least, it will be obvious to a ordinary skill of art to deliver the credential and the pass-phrase that is used to wrap the credential separately for the motivation of communication security.

Therefore, previous USC 103 type rejections of claims 1, 3-18, 20-29, 31-33 are maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that

Art Unit: 2136

the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 3-9, 17, 18, 20, 23, 29 are rejected under USC 103 (a) as being unpatentable over Lee et al ("A secure electronic software distribution (ESD) protocol based on PKC", EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Hypponen (US 6986050B2) further in view of Bathrick et al (US 5825300).

Regarding claim 1, Lee et al discloses a computer implemented system ((Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol) for processing credentials, comprising the following computer executable components:

- a wrapper (Figure 1,2: element: Electronic License Packaging; wrapped package) that packages credentials associated with resources of a service (Section 2.2, 3.1, 3.2; merchant server comprising an electronic license packaging module that wraps the software to be downloaded in a package);

- a pass phrase (a "secret" string shared only by authorization unit in client's computer and by the server) employed in connection with generation of the wrapper (Figure 1,2: element: generating electronic license Package; E license; deriving cryptographic digest, H from shared secret; cryptographic function H (part of the e-license) is used to lock/ unlock the wrapped package);

- the pass phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources to the server (Section 2.2,3.1,3.2; locked wrapper/ package software that can be unlocked using an Electronic License Certificate (ELC) containing a cryptographic digest derived from a "secret" component)

Lee et al does not disclose expressly

a pass phrase employed in connection with generation of cryptographic wrapping key,
the pass phrase distributed separately from the credentials.

However Hypponen discloses a pass phrase employed in connection with generation of cryptographic wrapping key (Fig 2, Claim 1; generating cryptographic key/ decryption key from passphrase),

Furthermore, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing key and certificate material separately).

Hypponen , Bathrick et al and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Hypponen and Bathrick et al with Lee et al for distributing the pass phrase separately from the credential and using a passphrase to generate the cryptographic wrapping key. Motivation for doing so would have been that such measures would provide a strong access control, and transmission security(Hypponen , Col 1, lines 15-35; Bathrick et al, Col 1, line 65 to col 2, line 4).

Regarding claim 18, it recites the limitations of claim 1, therefore, it is rejected applying as above rejecting claim1, furthermore, Lee et al discloses a method to facilitate a security connection between entities (Section 3: Proposed ESD Protocol), comprising:

generating a strong password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, passwd) [Lee et al discloses generation of an electronic license certificate comprising password];

generating a pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: generating E-license, secret) [Lee et al discloses generation of an electronic license certificate comprising a “secret” string. The “secret” is shared only between the authentication module and the server and is a random string.]

wrapping the password cryptographically via the pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, H(secret, customer_ID, passwd)) [Lee et al discloses generation of an electronic license certificate also comprising cryptographic function H that cryptographically wraps the password] ;

storing the wrapped password in an executable (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: merchant server, JDBC data source, electronic license processing) [Lee et al discloses use of JDBC component, a storing facility and “electronic license packaging” module (which contains password in it) to wrap the packaged software].

Lee et al does not disclose expressly

a pass phrase employed in connection with generation of cryptographic wrapping key, the pass phrase distributed separately from the credentials.

However Hypponen discloses a pass phrase employed in connection with generation of cryptographic wrapping key (Fig 2, Claim 1; generating cryptographic key/ decryption key from passphrase),

Furthermore, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing key and certificate material separately).

Regarding claim 3, it is rejected applying as above rejecting claim 1, furthermore, Lee et al discloses the credentials providing stronger encryption than the pass phrase (Section 3.1, 3.2) [Lee et al discloses that second component of the electronic license certificate (that implies to credentials) are encrypted by using a public key and server's private key; public key encryption is usually stronger (128 bit or more) than the random string.]

Regarding claim 4, it is rejected applying as above rejecting claim 3, furthermore, Lee et al teaches that credentials are encrypted with greater than 100 bits of encryption (Section 1: Introduction, Paragraph 3; Section 3.1, 3.2: Secure Installation scheme, Paragraph 1)[Lee et al teaches use of encryption schemes such as Diffie Hellman, RSA, MD5, and SHA – all of them usually use greater than 100 bits of encryption.

Regarding claim 5 and 9, Lee et al discloses a system of claim 3 (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme).

Lee et al does not disclose expressly that the pass – phrase having human readable, and alpha – numeric characteristics.

However, Hypponen discloses the pass – phrase having human readable, and alpha – numeric characteristics (Col 1, lines 40-65);

Regarding claim 6, 7, and 8, Lee et al discloses a system of one or more partners request access to the resources, or partners store and distribute the credentials (Fig 1, producer; merchant server).

Regarding claim 17, it is rejected applying as above rejecting claim 1, furthermore, Lee et al discloses a computer readable medium having computer executable instructions stored thereon to

Art Unit: 2136

perform at least one of processing and generation of the wrapper and the pass phrase (Section 2.2: Software based technologies; Section 3.1: Overall architecture; Figure 1, element: electronic license packaging) [Lee et al teaches use of JDBC component “electronic license packaging” to package and email the wrapped electronic license (which contains a “secret” string as pass phrase) to customer].

Regarding claim 20, it recites the limitation of claim 18, therefore, it is rejected applying as above rejecting claim 18, furthermore, although Lee et al discloses a pass phrase based encryption/ decryption mechanism to lock/ unlock a password (Page 65, lines 1-10; Page 67, Lines 1-15; Fig 2, element : E license; Fig 3, decryption of encrypted exe file; AA to unlock/ decrypt exe file using E license; E license comprising a hash digest containing “secret” and password; AA having “secret”; examiner interprets either a “secret” or a “private key” can be used to decrypt such encrypted executables or a wrapped password).

Regarding claim 23, it is rejected applying as above rejecting claim 18, furthermore, Lee et al discloses a method of limiting access to the executables (Section 2.2: Software based technologies; Section 3.3: Illegal copy protection mechanism; Figure 3: Illegal copy protection protocol using multi thread). [Lee et al teaches use of an authentication server to limit access to the executable packages]

Regarding claim 29, it is rejected applying as above rejecting claim 28, furthermore, Lee et al discloses a wrapper field being cryptographically weaker than the password (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme) [Lee et al discloses that password and other credentials in electronic license certificate are encrypted by using a public key and server’s private

key; public key encryption is usually stronger (128 bit or more) than the random string or the key crunching algorithm (usually 64 bit encryption) to generate random string from the pass phrase or a secret string]

7. Claims 10-12 are rejected under USC 103 (a) as being unpatentable over Lee et al ("A secure electronic software distribution (ESD) protocol based on PKC", EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Hypponen (US 6986050B2) further in view of Bathrick et al (US 5825300) further in view of Brainard (SecurSight: An architecture for secure information access, RSA Lab).

Regarding claim 10, 11, Lee et al does not disclose expressly use of that pass phrase over a SSL connection or in a VPN environment.

However, Brainard discloses use of that pass phrase over a SSL connection or in a VPN environment (Page 6, Col 1, step 5, application server, SSL connection)

Brainard and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Brainard with Lee et al for utilizing a pass phrase base wrapper for credential security in a system involving SSL connection or VPN. The motivation for doing so would been that a SSL connection/ secure communication channel, or VPN provides further content security while transmitted through a network.

Regarding claim 12 is rejected applied as above rejecting claim 11, furthermore Lee et al discloses issuing an Electronic License Certificate (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: certificate) by merchant server, and obtaining a public

key certificate from a third party Certificate Authority (Section 3.1: Overall architecture, Figure 1, element CA) to facilitate secure communication between merchant server and customer.

8. Claims 27,28,31,33 are rejected under USC 103 (a) as being unpatentable over Lee et al (“ A secure electronic software distribution (ESD) protocol based on PKC”, EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Bathrick et al (US 5825300).

Regarding claim 27, it recites the limitations of claims 1, and 18, therefore, it is rejected applying as above rejecting claims 1 and 18, furthermore, Lee et al discloses a computer executable system to facilitate a security relationship between parties (Section 3: Proposed ESD Protocol), comprising:

computer implemented means for generating a strong password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: generating E-license, passwd) [Lee et al teaches generation of an electronic license certificate comprising password in it];

computer implemented means for generating a pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: generating E-license, secret) [Lee et al discloses generation of an electronic license certificate comprising a secret string that works as a pass phrase];

computer implemented means for generating a package (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Figure 1, element: Electronic License Packaging) [Lee et al discloses a electronic license packaging module to package software in a wrapper]

Art Unit: 2136

computer implemented means for storing the password in the package (Section 3.1, 3.2; Figure 2, element: E-license, H(secret, customer_ID, passwd); Figure 1, element: merchant server, JDBC data source, electronic license processing);

computer implemented means for locking the package with the pass -phrase (Section 2.2: Software based technologies; Section 3.1, 3.2; Figure 1, element: merchant server, JDBC data source, electronic license processing) [Lee et al discloses a H function (as a part of electronic license certificate) comprising a pass phrase like "secret" string that is used to lock the wrapper containing packaged software].

Lee et al does not disclose expressly

Transmitting the package and the passphrase to a system via different communication medium.

However, Bathrick et al discloses transmitting the package and the passphrase to a system via different communication medium. (Col 2, lines 33-40, 64-67; Claim 1; distributing key and certificate material separately).

Bathrick et al and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Bathrick et al with Lee et al for distributing the pass phrase separately from the credential and using a passphrase to generate the cryptographic wrapping key. Motivation for doing so would have been that such measures would provide a strong transmission security (Bathrick et al, Col 1, line 65 to col 2, line 4).

Regarding claim 28, it recites the limitations of claim 27, therefore, it is rejected applying as above rejecting claim 27, furthermore, Lee et al discloses a computer readable medium having stored thereon a signal to communicate security data between at least two nodes (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme; Figure 1, element: electronic license packaging; figure 2: E license) comprising: a first data packet comprising:

A password component employed to establish a trust relationship between at least two nodes (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, Figure 2, element: E-license, $H(\text{secret}, \text{customer_ID}, \text{passwd})$) [Lee et al discloses an electronic license certificate which contains a cryptographic function $H(\text{secret}, \text{customer_ID}, \text{passwd})$ comprising password in it];

A wrapper field employed to encapsulate the password, the wrapper field mediating access to the password (Section 2.2: Software based technologies; Section 3.1, 3.2; Figure 1, element: Electronic license packaging; Figure 2, element: e-license) [Lee et al discloses generation of an electronic license certificate also comprising cryptographic function H that cryptographically wraps the password]

A second data packet comprising:

A pass phrase employed to generate (generating $H(\text{secret}, \text{customer_ID}, \text{passwd})$) and unlock the wrapper field (Page 65, lines 1-5; Page 67, lines 5-12; Fig 2, element: E license; Lee et al teaches employing an e-license comprising a “secret” to unlock the software package).

Lee et al does not disclose expressly

the pass phrase distributed separately from the credentials.

However, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing key and certificate material separately).

Regarding claim 31, Lee et al discloses a computer implemented system to establish a trust relationship, comprising the following computer executable components:

A wrapper generated by the service to package the credentials (Section 2.2: Software based technologies; Section 3.2: Overall Architecture; Figure 1, element: Electronic License Packaging, producer, merchant server)[Lee et al discloses a wrapper generated by merchant server (associated with a producer module) to package software];

A pass phrase employed to generate the wrapper and mediate access to the service (Section 2.2: Software based technologies; Section 3.2: Overall Architecture; Figure 1: Overall Architecture of proposed protocol) [Lee et al teaches a secret string within an electronic license certificate which is used to lock the wrapper containing packaged software, and such certificate is used to mediate access to the resources];

a service that controls one or more resources, the service issues credentials to facilitate access to the resources (Fig 1, merchant server, certificate authority, CA; Section 3.2; authentication server AA).

Lee et al does not disclose expressly the pass phrase distributed separately from credentials.

However, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing key and certificate material separately).

Regarding claim 33, it recites the limitations of claim 28, therefore, it is rejected applying as above rejecting claim 28, furthermore, Lee et al discloses a computer readable medium having stored

Art Unit: 2136

thereon a data structure (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Fig 2, element: e- license; Fig 3, element: executable packaged file, decryption of encrypted exe file and software execution thread), comprising:

A first data field containing cryptographic data associated with a password (Page 67, lines 1-18; Fig 2, element: E-license) [Lee et al teaches AA storing password data used to create a cryptographic hash digest];

A second data field (secret field of H function) containing cryptographic data associated with a pass phrase, the pass phrase employed to migrate exposure of the password to non trusted entitie (Page 67, lines 1-18; Fig 2, element: E-license) [Lee et al teaches AA storing “secret” data used to create a cryptographic hash digest];

A third data field containing a wrapper employed to encapsulate the password, the wrapper generated by the pass phrase (Page 67, lines 1-18; Fig 2, element: E-license containing H which generated by shared secret) [Lee et al teaches AA generating a cryptographic hash digest, H to encapsulate pass phrase and password];

Lee et al does not disclose expressly the wrapper distributed separately from the passphrase to facilitate a security connection between entities.

Bathrick et al discloses the wrapper distributed separately from the passphrase to facilitate a security connection between entities (Col 2, lines 33-40, 64-67; Claim 1; distributing key and certificate material separately).

9. Claims 13 –16, 21-22, 24-25, 32 are rejected under 35 USC 103 (a) as being unpatentable over Lee et al (“ A secure electronic software distribution (ESD) protocol based on PKC”, EC-Web 2000,

Art Unit: 2136

LNCS 1875, pp. 63-71, 2000) in view of in view of Hypponen (US 6986050B2) further in view of Bathrick et al (US 5825300) further in view of Brainard ("SecurSight: An overview for secure information access", RSA Laboratories).

Regarding claim 13 and 14, Lee et al discloses a system of claim 1 (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).

Lee et al does not disclose expressly a platform provisioning service, or such service being associated with a partner including a service provider and tenant.

However, Brainard teaches a platform provisioning service, or such service being associated with a partner including a service provider and tenant (Fig 5, PAC; SecurSight authentication service; system consist of manager, desktop, and application server; Brainard's enterprise network resources and applications imply capability of performing billing, financial, or accounting functions) .

Brainard, and Lee et al are analogous art because they are from the same field of endeavor of transmission and access of secure information. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Brainard with Lee et al for designing system of claim 1 further comprising platform provision service, partners, and service providers in order to facilitate network or enterprise application/ resources to the users efficiently and securely.

Regarding claim 15 is rejected applied as above rejecting claim 14, furthermore Lee et al discloses a "secret" string as a part of Electronic License Certificate (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: certificate) that is used to

unlock credentials and achieve access to the services (Section 2.2: Software based technologies, Paragraph 1;Section 3.2: Secure Installation scheme, Paragraph 2) .

Regarding claim 16 is rejected applied as above rejecting claim 14, furthermore Lee et al discloses a system associated with ecommerce technology (Section 1: Introduction, Paragraph 1 and 2) and use web browser to present the credentials to the client (Section 4: Comparison with existing models, Table 1) that is used to unlock credentials and achieve access to the services (Section 2.2: Software based technologies, Paragraph 1;Section 3.2: Secure Installation scheme, Paragraph 2).

Regarding claim 21, Lee et al discloses a system of claim 18.

Lee et al does not expressly teaches requesting a secure socket layer (SSL) connection or presenting an SSL certificate in response to the request.

However, Brainard teaches requesting a secure socket layer(SSL) connection (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service) and presenting an SSL certificate in response to the request(Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches a desktop requesting for SSL connection with application server, and presenting a certificate to certificate validation service for validation.]

Regarding claim 22 is rejected applied as above rejecting claim 21, furthermore Brainard teaches a method comprising at least one of:

Verifying an SSL certificate (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches an application access agent and a certificate validation service to validate SSL certificates];

Requesting a Universal Resource Locator (URL) from a listener(Section 2.4: Comparison with other authenticators)[Brainard teaches obtaining web browser based credentials which essentially refers to use of an URL] ;

Presenting authentication credentials to a receiver (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches desktop presenting a certificate to be validated by the certificate validation service.];

Logging in a caller to an account (Section 3.1: PAC definition; Section 3.3: use of PACs by connect agents) [Brainard teaches a connect agent that initiates a client's access to an account after certificates are validated].

Regarding claim 24, Brainard teaches the method comprising at least one of: setting up account privileges; designating account contacts; and verifying contacts (Page 7, Col 1, Table 2, EAR; access right).

Regarding claim 25 is rejected applied as above rejecting claim 24. Furthermore, Lee et al does not expressly discloses a method of verbally communicating the password. However, Bathrick et al discloses a method comprising verbally communicating the password (Claim 3; non electronic communication medium for keying material/ password).

Regarding claim 32, it is rejected applying as above rejecting claim 31, furthermore, Brainard discloses a manager module that perform as provisioning service, and issues credentials to

Art Unit: 2136

authenticate users to access resources (Section 1.1: SecurSight Design Principal; Section 1.2: Component; Section 3: Authorization; Figure 5: PAC Usage).

Conclusion

10. **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

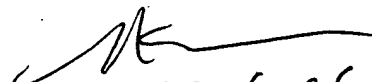
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551, fax number is 571-273-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, A.U. 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


12,6106